(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 41 038 A 1**

(51) Int. Cl.[6]:
G 07 F 7/08
G 06 K 19/07
// G07B 15/00

(21) Aktenzeichen: P 44 41 038.7
(22) Anmeldetag: 18. 11. 94
(43) Offenlegungstag: 23. 5. 96

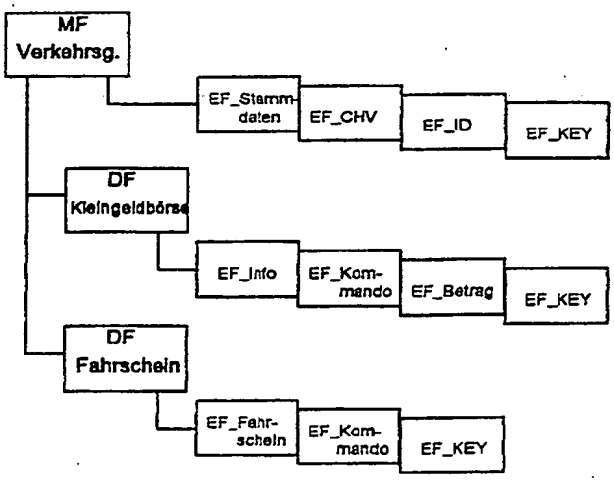
DE 44 41 038 A 1

(71) Anmelder:
Deutsche Telekom AG, 53175 Bonn, DE

(72) Erfinder:
Hartleif, Siegfried, 64823 Groß-Umstadt, DE

(54) Verfahren zum Erwerb und Speichern von Berechtigungen mit Hilfe von Chipkarten

(57) Die Erfindung bezieht sich auf ein Verfahren zum Erwerb, Speichern und Überprüfen von Berechtigungen mit Hilfe von Chipkarten. Auf der Chipkarte befindet sich mindestens ein Speicherbereich, der bei Bezahlung einer Berechtigung mit der erworbenen Berechtigung belegt wird.
Die Bezahlung der Berechtigung erfolgt entweder intern durch eine Belastung der Kleingeld- oder Kreditbörse der Chipkarte oder extern mit Bargeld oder Kreditkarte.



DE 44 41 038 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 03. 96 802 021/154

DOCID: <DE___4441038A1_I_>

Beschreibung

Die erfindungsgemäße Lösung bezieht sich auf ein Verfahren, mit dem Berechtigungen mit Hilfe einer Chipkarte erworben und zugleich auf dieser fälschungssicher abgespeichert werden können.

Dabei sind generell 3 Verfahren anwendbar

1. Der Kunde weist sich mit Hilfe seiner Chipkarte aus und erwirbt die Berechtigung.
Bei diesem Verfahren wird mit Hilfe der Chipkarte ein Verrechnungsdatensatz erzeugt, der zu einer Clearingstelle bzw. zur Bank des Kunden weitergereicht wird und dort zur Belastung des Kundenkontos führt. Die erworbene Berechtigung wird in der Chipkarte fälschungssicher gespeichert und kann zu Kontrollzwecken ausgelesen werden. Dieses Verfahren eignet sich vor allem zum Erwerb von höherpreisigen Berechtigungen wie z. B. Flugtikket, Zeitkarten für den öffentlichen Personalverkehr. Der Kunde benötigt eine Kreditbörsen- bzw. elCash-Funktion auf seiner Chipkarte.
2. Der Kunde hat eine Kleingeldbörse mit entsprechendem Guthaben auf seiner Chipkarte.
Bei diesem Verfahren wird der Betrag zum Erwerb der Berechtigung aus der Chipkartenbörse herausgebucht. Die Berechtigung selber wird dann wie unter 1. abgespeichert. Dieses Verfahren eignet sich vor allem zum Erwerb von niederpreisigen Berechtigungen, wie z. B. Eintrittsberechtigung Schwimmbad, Parkticket, Einzelfahrschein im öffentlichen Nahverkehr. Der Kunde benötigt eine Kleingeldbörse auf seiner Chipkarte.
3. Der Kunde kauft sich eine Berechtigung mit Geld bzw. mit Hilfe einer separaten Kreditkarte oder Eurocheckkarte.

Bei diesem Verfahren wird nur wie unter 1 die Berechtigung auf der Chipkarte abgespeichert.

Bekannt sind bereits folgende Grundlagen:
Architektur von Chipkarten und Kommandos für Chipkarten, die es erlauben, entsprechende Datenfehler für Berechtigungen anzulegen und damit zu arbeiten. ISO/IEC CD 7816-4.2 "Identification Cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange"
Börsen für Chipkarten
Auch Börsenfunktionen für Chipkarten werden zur Zeit von der Normung spezifiziert, z. B. CEN/TC224/WGIO, Draft prENxxxxx "Identification cards systems — Intersector electronic purse".

Zudem gibt es zahlreiche nationale und internationale Implementierungen, wie z. B. die Telekom-Börse, Börse auf der Karte der Berliner Verkehrsbetriebe, das MONDEX-System etc.

Kreditbörsen bzw. elCash-Funktionen auf Chipkarten Ein Konzept zum Erwerb von Waren bzw. Serviceleistungen per elCash ist im MFC-Konzept der GTI-Kooperation beschrieben (GAD, Telekom, IBM).

Erwerb von Fahrscheinen mit Hilfe von Chipkarten Auch hier sind zahlreiche Verfahren bekannt, wie z. B. Feldversuch der Telekom mit den Kieler Verkehrsbetrieben, Pilotversuch der Berliner Verkehrsbetriebe, Feldversuch in Biehl (Schweiz).

Bei allen bekannten Lösungen zum Erwerb von Berechtigungen mit Hilfe von Chipkarten wird jedoch davon ausgegangen, daß der Kunde die Berechtigung in Form von z. B. Quittungen, Fahrschein, Monatskarte, Parkmarke, Eintrittskarte etc. ausgehändigt bekommt. In den meisten Fällen wird der Beleg aber lediglich zu Kontrollzwecken und nicht aus abrechnungstechnischen Gründen (z. B. Beleg fürs Finanzamt) benötigt, das heißt der Kunde wirft den Beleg anschließend fort. Es reicht, gerade beim Erwerb von Einzelberechtigungen (z. B. Einzelfahrschein) aus, nur auf ausdrücklichen Wunsch des Kunden einen Papierbeleg auszugeben.

Der Erfindung liegt die Aufgabe zugrunde, die Möglichkeit einer Chipkarte für die Kombination von Bezahlvorgang und Abspeicherung der erworbenen Berechtigung zu nutzen. Damit braucht der Kunde nicht mehr länger die doch leicht zu verlierenden Belegzettel aufzuheben. Sinn macht diese Erfindung vor allem bei der Realisierung auf sogenannten City-Cards. Mit einer City-Card sollen Dienstleistungen unterschiedlicher Service-Anbieter einer Stadt genutzt werden können. Nach dem Erwerb der Berechtigung macht es Sinn, diese sogleich als elektronische Berechtigung auf der Karte zu speichern, wie z. B. als Zehner-Karte für das Schwimmbad, als Monatskarte für den Bus oder als Jahreskarte für den botanischen Garten etc.

Erfindungsgemäß verfügt die Chipkarte über einen Speicherbereich für eine Kleingeldbörse bzw. für eine Kreditbörsenfunktion.

Zudem können beliebig viele Speicherbereiche (begrenzt durch die Speicherkapazität der Karte) für das Ablegen der Berechtigungen vorgesehen werden.

Beim Erwerb der Berechtigungen mit Hilfe der Kleingeldbörse wird zunächst der Kaufpreis aus der Börse abgebucht. Dieser Vorgang muß kryptographisch abgesichert erfolgen. Das heißt, die Karte muß sich mit Hilfe von kryptographischen Verfahren von der Echtheit des Systems überzeugen. Desgleichen muß sich das System ebenfalls mit Hilfe von kryptographischen Verfahren von der Echtheit der Chipkarte überzeugen.

Es empfiehlt sich, auch den Abbuchungsvorgang selber kryptographisch zu sichern, damit nicht Beträge manipuliert bzw. die Börse mißbräuchlich entladen werden kann.

Das Abbuchen selber erfolgt mit einem Kommando "Abbuchen", das vom System an die Chipkarte gesendet wird. Die Karte reagiert mit einer Antwort an das System, in dem sie das ordnungsgemäße Reduzieren den Börsenbetrages bestätigt. Die Antwort ist zugleich Grundlage für einen sogenannten "Verrechnungsdatensatz", der über Terminal und Hintergrundsystem geführt wird und zu einer Gutschrift auf das Konto des Berechtigungsanbieters sowie einer Lastschrift auf das Konto des Börsenbetreibers führt. Nach Erhalt dieser Antwort lädt das System die Berechtigung in einen entsprechenden Speicherbereich der Chipkarte.

Auch dieser Vorgang muß kryptographisch gesichert verlaufen, damit keine manipulierten Berechtigungen abgelegt werden können und der Erwerb der Berechtigung zu jedem Zeitpunkt zweifelsfrei validiert werden kann.

Wird die Berechtigung mit Hilfe einer Kreditbörsen- oder elCash-Funktion der Chipkarte erworben, muß anstatt des Abbuchungskommandos ein Kommando an die Karte geschickt werden, das entsprechende Daten aus der Kreditbörse anfordert, wie z. B. Kartennummer, Name des Kontoinhabers, ggf. BLZ und Kto.Nr. des Karteninhabers.

Die Daten sind Grundlage eines Verrechnungsdatensatzes, der kryptographisch abgesichert durch das System geschickt wird und zu einer Belastung des Kundenkontos sowie zu einer Gutschrift auf das Konto des

Berechtigungsanbieters führt. Nach Erhalt der Daten aus der Kreditbörse lädt das System die Berechtigung, wie oben beschrieben auf die Chipkarte.

Wird die Berechtigung durch Bezahlen mit Bargeld, Kreditkarte, Euroscheck erworben, kann diese unmittelbar nach Erhalt des Bargeldes bzw. positiver Bearbeitung der Kreditkarte oder Euroscheckkarte wie oben beschrieben auf die Karte geladen werden.

Anhand eines Beispieles soll die erfindungsgemäße Lösung näher erläutert werden.

Beschreibung der Chipkarte:

Vorzugsweise handelt es sich um eine sogenannte Mulifunktionale Chipkarte, mit der es möglich ist, unterschiedliche Funktionen/Anwendungen von unterschiedlichen Service-Anbietern zu nutzen. Die unterschiedlichen Anwendungen werden im variablen Speicherbereich des Chips abgelegt und mit Hilfe des Betriebssystems verwaltet.

Eine mögliche Architektur des variablen Speicherbereiches für eine Karte, die die erfindungsgemäße Lösung unterstützt, ist in **Abb. 1** dargestellt. Herausgeber einer solchen Karte könnten z. B. Verkehrsgesellschaften sein.

Dem Hauptverzeichnis (MF) sind einzelne Datenfehler (EF) zugeordnet, die allgemeingültige Daten der Karte beinhalten. So sind im Datenfeld EF_Stammdaten z. B. die Kundendaten des Karteninhabers eingetragen oder im Datenfeld EF_CHV die persönliche Geheimnummer des Kunden.

Ausgehend vom Hauptverzeichnis sind die Unterverzeichnisse angeordnet, die die einzelnen Anwendungen/Funktionen mit den zugehörigen Datenfeldern beinhalten.

Im Beispiel enthält die Karte die Anwendungen "Kleingeldbörse" und "Fahrschein".

Ablauf

1. Der Kunde wählt am Fahrscheinautomaten das vorgesehene Fahrziel und bekommt den Fahrpreis per Displayanzeige mitgeteilt.
2. Der Kunde führt seine Chipkarte in den Kartenleser des Automaten ein.
3. Der Automat selektiert zunächst die Anwendung "vorausbezahlte Börse" und überzeugt sich von der Echtheit der Börse.
Er schickt eine Zufallszahl an die Karte und erhält diese mit dem Authentifikationsschlüssel verschlüsselt, zurück.
Er rechnet das von der Karte erhaltene Kryptogramm nach. Im Falle einer Übereinstimmung sieht er die Börse als echt an. Weiterhin überzeugt sich der Automat, daß die Börse über genügend Guthaben verfügt und das Gültigkeitsdatum nicht abgelaufen ist.
4. Die Karte überzeugt sich von der Echtheit des Automaten. Sie schickt eine Zufallszahl an den Automaten und erhält diese mit dem Authentifikationsschlüssel verschlüsselt, zurück. Sie rechnet das vom Automaten erhaltene Kryptogramm nach. Im Falle einer Übereinstimmung sieht sie den Automaten als echt an.
5. Der Automat schickt ein Abbuchungskommando an die Karte, das den abzubuchenden Betrag sowie einen MAC (Massage Authentification Code) über den Betrag enthält. Damit soll verhindert werden, daß der Betrag auf der Schnittstelle zur Karte manipuliert wird.
6. Die Karte reduziert den im Datenfeld EF_Betrag eingetragenen Betrag und sendet als Antwort eine MAC-gesicherte Quittung über den abgebuchten Betrag. Der Automat verifiziert die empfangene Quittung und schickt diesen als Verrechnungsdatensatz weiter an das Hintergrundsystem. Der Verrechnungsdatensatz führt schließlich zu einer Gutschrift auf dem Konto des Automatenbetreibers sowie zu einer Lastschrift auf dem Konto des Börsenbetreibers.
Nach der Verifikation der Quittung aus der Kleingeldbörse lädt der Automat den elektronischen Fahrausweis in das dafür vorgesehene Datenfeld. Das Ladekommando für den elektronischen Fahrausweis enthält die für einen Fahrausweis üblichen Daten wie Fahrpreis, Nr. des Fahrkartenautomates, Fahrziel, Gültigkeit etc. Alle Daten sind mit einem MAC gesichert.
7. Die Chipkarte übernimmt den Datensatz, legt diesem MAC-gesichert im Datenfeld EF_Fahrschein ab und sendet anschließend eine positive Quittung an den Automaten.
8. Der Datensatz kann zur Kontrolle jederzeit ausgelesen werden. An Hand des MACs kann ein Kontrolleur überprüfen, ob die Fahrscheindaten nicht manipuliert wurden.

Patentansprüche

1. Verfahren zum Erwerb, Speichern und Überprüfen von Berechtigungen mit Hilfe von Chipkarten, **dadurch gekennzeichnet,**
daß sich mindestens ein Speicherplatz für Berechtigungen auf der Chipkarte befindet,
daß durch Bezahlung der Berechtigung mit Hilfe einer internen Bezahlfunktion ein Speicherplatz der Chipkarte mit der erworbenen Berechtigung belegt wird,
daß durch Bezahlung der Berechtigung mit Hilfe einer externen Bezahlfunktion ein Speicherplatz der Chipkarte mit der erworbenen Berechtigung belegt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Bezahlung durch die interne Bezahlfunktion durch eine Belastung der Kleingeld- oder Kreditbörse der Chipkarte erfolgt.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Bezahlung durch die externe Bezahlfunktion mit Kreditkarte oder durch Bargeld erfolgt.
4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß bei Bezahlung der Berechtigung mit einer internen Bezahlfunktion ein Verrechnungsdatensatz von der Chipkarte erzeugt wird.
5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß dieser Verrechnungsdatensatz bei Bezahlung aus der Kreditbörse über das Terminal und ein Hintergrundsystem beim Berechtigungsanbieter und beim Kunden einen Buchungsvorgang auslöst.
6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß dieser Verrechnungsdatensatz bei Bezahlung aus der Kleingeldbörse über das Terminal und ein Hintergrundsystem beim Berechtigungsanbieter und beim Börsenbetreiber einen Buchungsvorgang auslöst.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 44 41 038 A1
Int. Cl.[6]: G 07 F 7/08
Offenlegungstag: 23. Mai 1996

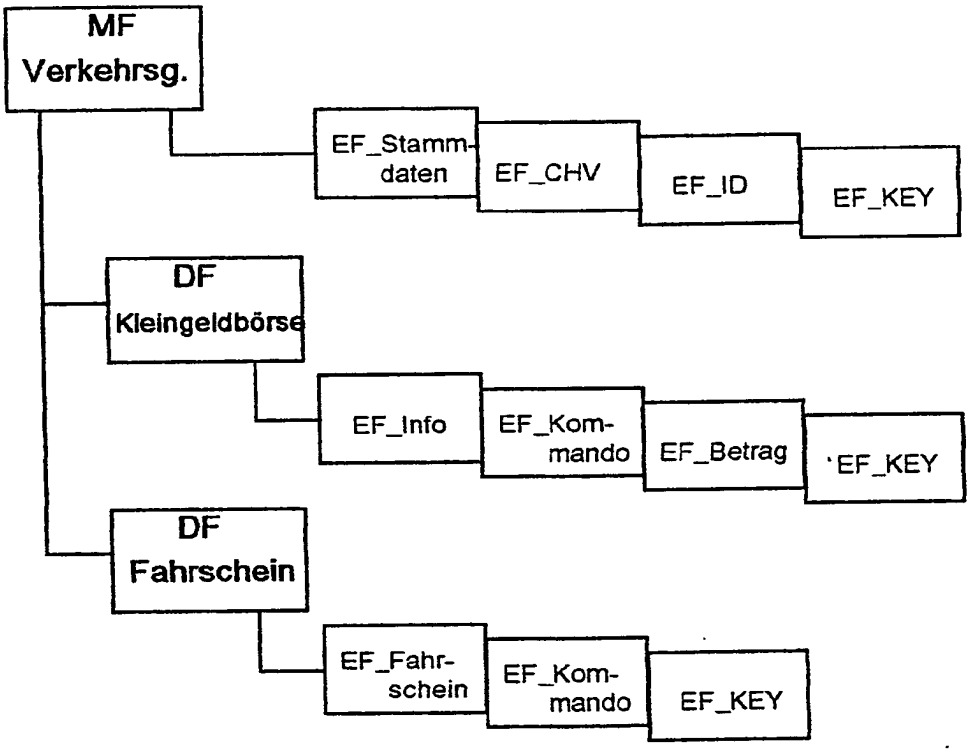


Abb.1